**Dirección General de Tecnologías y Desarrollo Digital**

# Informe de Auditoría Interna

## Criterios de auditoría:

**ISO 9001**

- Fecha de la última auditoría externa
- Hallazgos de auditorías internas/externas recientes (año anterior).
- Impacto en la operación del Sistema Integral de Calidad.
- Cambios críticos en el proceso/subproceso hechos recientemente.

**ISO 20000**

- Fecha de la última auditoría externa
- Hallazgos de auditorías internas recientes (año anterior)
- Servicios próximos a certificar
- Antigüedad de servicio certificado

**ISO 27001**

- Auditorías externas previas
- Hallazgos de auditorías internas recientes (año anterior)

**CONTROLES DE SEGURIDAD (ANEXO A)**

- Criticidad del control de seguridad de la información
- Implementación por el personal
- Cambios recientes o hallazgos

## Periodo de auditoría:

18, 19, 20 y 21 de abril 2023.

## Alcance:

Sistema de Integral de Calidad (Sistema de Administración de Calidad, Sistema de Administración de Servicios y Sistema de Administración de Seguridad de la Información).

## Clasificación de hallazgos:

C: Cumple.
NC: No conformidad.
OM: Oportunidad de mejora.
N/A: No aplica.

## Procesos considerados con base al Plan Estratégico de Auditorías Internas:

Los establecidos en la Planeación 2023, dentro del DOI-011 Planeación estratégica de auditorías internas. El subproceso de Seguridad de la Información SP-SER-019 se eliminó posterior a la liberación del plan 2023.

| No. | Alcance | Clasificación del hallazgo | Requisito | Descripción del Hallazgo | Folio de Acción Correctiva |
|---|---|---|---|---|---|
| 1 | ISO 27001 | NC | 8.1 Planteamiento operacional y control (impacto en el 8.2 y 8.3) | **Requisito incumplido**: La organización deberá controlar los cambios planificados y revisar las consecuencias de cambios involuntarios tomando acción a mitigar de algunos efectos adversos.<br><br>**Hallazgo encontrado**: Durante la auditoría se detecta que se tiene un inventario de activos, sin embargo, debido a los cambios organizacionales que se han presentado recientemente en la Dirección, es necesario actualizar el inventario de acuerdo a las funciones y el personal nuevo, ya que los activos que se identifican sirven como base para la elaboración de una efectiva identificación, evaluación y tratamiento de riesgos de seguridad.<br><br>**Evidencia objetiva:** RC-04-009 Inventario de activos. | 05-01/23 |
| 2 | ISO 9001 | NC | 8.1 Planteamiento operacional y control | **Requisito incumplido**: La organización debe planificar , implementar y controlar los procesos necesarios para cumplir los requisitos para la provisión de productos y servicios, y para implementar las acciones determinadas, mediante: d) la implementación del control de los procesos de acuerdo con los criterios<br><br>**Hallazgo encontrado**: Durante la auditoría se detecta que se llevan a cabo proyectos y seguimientos especiales, los cuales se gestiona el estatus y avance por medio de la herramienta de portafolio de proyectos, sin embargo, al revisarlos con los administradores se visualiza que existen seguimientos especiales con estatus "abierto" que ya fueron cerrados con el usuario. Así como también existen iniciativas con más de 50 meses con el estatus de "en espera" y proyectos con documentación no realizada o desactualizada (Matriz de Riesgos, Bitácora de Asuntos Pendientes, entre otros).<br><br>**Evidencia objetiva:** proyectos 579, 955, 18, seguimientos 969, Iniciativas 362, 363 (se establece una muestra, sin embargo, se revisaron todos los que tenía cada administrador de proyecto). | 05-02/23 |

| No. | Alcance | Clasificación del hallazgo | Requisito | Descripción del Hallazgo | Folio de Acción Correctiva |
|---|---|---|---|---|---|
| 3 | ISO 27001 | OM | A6.2.2 | Durante la auditoría se detecta que hay bajas de personal y se tiene en regla la documentación, sin embargo, no existen notificaciones oficiales de dichas bajas, por lo que se deberá definir un mecanismo/ procedimiento de comunicación para que la actualización de las cuentas sea más efectiva.<br><br>**La evidencia que lo soporta:** Se cuenta con una política para opciones de teletrabajo DOI-105 Rev.04-03/23, se mostró evidencia de los siguientes folios:<br>• 137118: Acceso a VPN<br>• 137108: Escritorio remoto<br>• 136458<br>Se tiene un inventario de accesos remotos RC-04-004 Rev. 02-12/22 actualizado a marzo 2023. | No aplica |
| 4 | ISO 27001 | OM | A12.4.3 | Durante la auditoría se mostró que existe una lista de usuarios con privilegios de administrador, sin embargo, no se tiene una frecuencia definida de validación de los mismos, en relación a los accesos a los servidores, además es necesario mostrarlo en el formato RC-04-015.<br><br>**La evidencia que lo soporta:** Se mostró un reporte a febrero 2023, archivo con nombre lista admin, listando los administradores o que están en grupo de administrador de servidores. | No aplica |
| 5 | ISO 27001 | OM | A16.1.3<br>A 16.1.6 | Durante la auditoría, se detectó en el DOI-149 Gestión de Incidentes de Seguridad con Rev.02-03/23, que describe en "actividades posts incidentes": se deberá documentar estos incidentes y las lecciones aprendidas de los mismos, a través del subproceso de mejora continua y el subproceso de lecciones aprendidas, sin embargo, actualmente se gestiona de otra manera que ha resultado efectiva, por lo que, se tendrá que actualizar el DOI. Adicional, es necesario enriquecer la documentación de los cambios realizados después de un incidente de seguridad para la generación de conocimiento después del cierre del incidente.<br><br>**La evidencia que lo soporta:** Se mostró el reporte de vulnerabilidades técnicas RC-04-019, con las vulnerabilidades reportadas. Se mostró la herramienta ITIR donde se centraliza los seguimientos de los incidentes. | No aplica |

**Firmas de aprobación**

| | | |
|---|---|---|
| **Ing. Ana Victoria Alvarez Quiroz**<br>**Representante de ISO 9001** | **Ing. Graciela C. Flores Reyes**<br>**Representante de ISO 20000** | **Lic. Jesús Cortés Hernández**<br>**Representante de ISO 27001** |
| **Dr. Mario Alberto González de León**<br>**Director** | | |